



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,832	06/30/2003	Art Shelest	13768.344	3053
47973 7590 05/11/2007 WORKMAN NYDEGGER/MICROSOFT 1000 EAGLE GATE TOWER 60 EAST SOUTH TEMPLE SALT LAKE CITY, UT 84111			EXAMINER CERVETTI, DAVID GARCIA	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 05/11/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/611,832

Applicant(s)

SHELEST ET AL.

Examiner

David G. Cervetti

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 February 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 12, 14-22, 34 and 36-60 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 12, 14-22, 34 and 36-60 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's arguments filed February 16, 2007, have been fully considered but they are not persuasive.
2. Claims 12, 14-22, 34, and 36-60 are pending and have been examined. Claims 1-11, 13, 23-33, and 35 have been cancelled.

Response to Amendment

3. The rejection of claims 1 and 23 under 35 U.S.C. 112, first paragraph, is withdrawn.
4. The rejection of claims 23-44 under 35 U.S.C. 101 is withdrawn.
5. Regarding Applicant's arguments that Checkpoint does not teach "generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall", Examiner respectfully submits and points Applicant's attention to page 32 of Checkpoint AA, where the security server generates the credential going to the server (final destination) which sees it as coming from the security server (gateway). **Applicant's arguments are not persuasive.**

Claim Objections

6. Claim 36 is objected to because of the following informalities: "wherein the are related to at least one of a". Appropriate correction is required.
7. Claim 38 is objected to because of the following informalities: "of claim 35". Appropriate correction is required.
8. **This is not intended to be a complete list of such informalities.**

Claim Rejections - 35 USC § 102

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. **Claims are rejected under 35 U.S.C. 102(b) as being anticipated by Check Point (NPL “Check Point FireWall-1 User Guide”, books “Architecture and Administration” – AA, and “Virtual Private Networking with Check Point FireWall-1” – VP, hereinafter Checkpoint).**

Regarding claims 45 and 58, Checkpoint teaches

- in a private network comprising a server and a firewall, which acts as a gateway by controlling access to the server, a method of providing access to the server through the firewall without a client knowing about the firewall (**AA, chapter 1, pp. 28-41**), the method comprising the acts of:
 - receiving at the firewall, an access request from the client that is directed to the server because the client does not know that the firewall operates as a gateway for the server (**AA, chapter 1, pp. 27-29**);
 - generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall (**AA, chapter 1, pp. 28-34**);
 - the firewall sending a request for the client to authenticate to the firewall, the request including the one or more firewall authentication credentials so that the client knows of the level of trust between the server and the

firewall without having to make a separate request (**AA, chapter 1, pp. 35-39**);

- receiving at the firewall, one or more authentication credentials from the client (**AA, chapter 1, pp. 27-39**);
- the firewall verifying the one or more client authentication credentials (**AA, chapter 1, p. 28**); and
- thereafter, allowing the client to access the server through the firewall (**AA, chapter 1, p. 28**).

Regarding claims 46, Checkpoint teaches establishing a secure connection between the firewall and the server; and forwarding data received from the client to the server over the secure connection (**AA, chapter 1, pp. 27-33**).

Regarding claim 47, Checkpoint teaches receiving at the firewall data from the client; the firewall signing the received data; and the firewall forwarding the signed data to the server (**VP, chapter 1, pp. 7-13**).

Regarding claim 48, Checkpoint teaches wherein the private network resource is one of a host, gateway or server (**AA, chapter 1, pp. 27-33**).

Regarding claim 49, Checkpoint teaches wherein the client is a second firewall (**AA, chapter 1, pp. 27-29**).

Regarding claim 50, Checkpoint teaches wherein the client maintains a separate connection with another server (**VP, chapter 1, pp. 11-13**), and wherein only data intended for the private network passes through the firewall (**AA, chapter 1, pp. 27-33**).

Regarding claim 51, Checkpoint teaches wherein the other server is part of a separate and distinct virtual private network (**VP, chapter 2, pp. 15-32**).

Regarding claims 53 and 60, Checkpoint teaches

- wherein the act of generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall comprises an act of generating one or more credentials that permit the firewall to unilaterally authenticate with the client such that the client does not need to have further communications with the firewall to authenticate the firewall (**AA, pp. 69-85**).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. **Claims 12, 14-22, 34, 36-44, and 54-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Checkpoint, and further in view of Boroditsky et al. (US Patent 6,332,192, hereinafter Boroditsky).**

Regarding claims 12 and 34, Checkpoint teaches

- in a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a method of establishing a connection to the private network resource while balancing authentication processing requirements

between a client and the firewall to mutually guard against denial of service attacks, the method comprising steps for **(AA, chapter 1, pp. 28-41)**:

- receiving an assertion from the client that the client has credentials appropriate for accessing the private network resource (AA, chapter 1);
- initiating a series of authentication transactions between the client and the firewall, the series of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein successful completion each authentication transaction incrementally increases a level of trust between the client and the firewall (AA, chapter 1, pp. 28-48).

Checkpoint does not expressly disclose for each of the series of authentication transactions between the client and the firewall: sending a challenge to the client, the correct answer to the challenge obtainable from the asserted credentials without having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer; receiving a response from the client including an answer to the challenge; and verifying whether or not the answer included in the response the correct answer to the challenge; and when an acceptable level of probability that the client actually possesses the asserted credentials

is reached based on a plurality of correct answers, the firewall granting the client access to the private network resource through the firewall.

However, Boroditsky teaches for each of the series of authentication transactions between the client and the firewall: sending a challenge to the client, the correct answer to the challenge obtainable from the asserted credentials without having to divulge the asserted credentials such that if the client actually possesses the asserted credentials the client can generate the correct answer; receiving a response from the client including an answer to the challenge; and verifying whether or not the answer included in the response the correct answer to the challenge; and when an acceptable level of probability that the client actually possesses the asserted credentials is reached based on a plurality of correct answers, the firewall granting the client access to the private network resource through the firewall (col. 11, lines 15-67, col. 12, lines 1-10).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the authentication method disclosed by Boroditsky with the system of Checkpoint.

One of ordinary skill in the art would have been motivated to perform such a modification to further protect access to secure resources **(cols. 1-2).**

Regarding claims 14 and 36, the combination of Checkpoint and Boroditsky teaches wherein the answers are related to at least one of a user's name, client's IP address, password, passport, smart-card or credit card number **(Checkpoint, AA, chapter 1, pp. 27-33).**

Regarding claims 15 and 37, the combination of Checkpoint and Boroditsky teaches wherein a challenge is a question, and wherein one or more client credentials received is an answer to the question (**Checkpoint, AA, chapter 1, pp. 29-33**).

Regarding claims 16 and 38, the combination of Checkpoint and Boroditsky teaches wherein once the client is granted access to the private network resource the only data passed through the firewall from the client are those packets of data destined to the private network resource (**Checkpoint, AA, chapter 1, pp. 27-33**).

Regarding claims 17 and 39, the combination of Checkpoint and Boroditsky teaches establishing an authenticated channel between the firewall and the private network resource, wherein the authenticated channel is established through signing the data from the firewall (**Checkpoint, VP, chapter 1, pp. 7-13**).

Regarding claims 18 and 40, the combination of Checkpoint and Boroditsky teaches discarding any unsigned packets of data received by the private network resource (**Checkpoint, VP, chapter 1, pp. 7-13**).

Regarding claims 19 and 41, the combination of Checkpoint and Boroditsky teaches wherein the private network resource is one of a host, gateway or server / wherein the server comprises a host or a gateway (**Checkpoint, AA, chapter 1, pp. 27-33**).

Regarding claims 20 and 42, the combination of Checkpoint and Boroditsky teaches wherein the client is a second firewall (**Checkpoint, AA, chapter 1, pp. 27-29**).

Regarding claims 21 and 43, the combination of Checkpoint and Boroditsky teaches establishing a connection with another resource of a separate private network

while simultaneously maintaining a secured channel between the firewall and the client
(Checkpoint, VP, chapter 1, pp. 11-13).

Regarding claims 22 and 44, the combination of Checkpoint and Boroditsky teaches establishing a connection with another private network resource while simultaneously maintaining a secured channel between the firewall and the client
(Checkpoint, VP, chapter 1, pp. 11-13).

Regarding claims 54 and 56, the combination of Checkpoint and Boroditsky teaches wherein the step for initiating a series of authentication transactions between the client and the firewall comprises an act of initiating a sequence of exchanges of an interactive proof protocol **(Boroditsky, col. 11, lines 15-67, col. 12, lines 1-10).**

Regarding claims 55 and 57, the combination of Checkpoint and Boroditsky teaches wherein for each of the series of authentication transactions sending a challenge to the client comprises sending a challenge that includes: a portion of a prior response received from the client; and a series of random questions, correct answers to the random questions obtainable by the client if the client actually possesses the asserted credentials **(Boroditsky, col. 11, lines 15-67, col. 12, lines 1-10).**

13. Claims 52 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Checkpoint.

Regarding claims 52 and 59, Checkpoint does not expressly teach trust between server and firewall, however it does teach trusted communications **(public keys and certificate authority, AA, pp 116-119)** between a management station and the firewall (gateway). Therefore, it would have been obvious to one having ordinary

Art Unit: 2136

skill in the art at the time the invention was made to extend the use of digital certificates to other servers/terminals within the network that connection to the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to provide trusted communication between all parties and to provide confidentiality, integrity, and availability (AA, pp. 112-117).

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.


Art Unit: 2136

16. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

17. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


5,9107